METHOD AND SYSTEM FOR REDUCING THE FALSE ALARM RATE OF NETWORK INTRUSION DETECTION SYSTEMS

ABSTRACT OF THE DISCLOSURE

According to one embodiment of the invention, a computerized method for reducing the false alarm rate of network intrusion detection systems includes receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host and identifying characteristics of the alarm from the data packets. The characteristics include at least an attack type and an operating system fingerprint of the target host. The method further includes identifying the operating system type from the operating system fingerprint, comparing the attack type to the operating system type, and indicating whether the target host is vulnerable to the attack based on the comparison.